Universidade Federal do Rio de Janeiro

Núcleo de Computação Eletrônica

Patrick Martins Mendes

GOVERNANÇA DA SEGURANÇA: A Segurança da Informação alinhada aos Negócios

Rio de Janeiro

2008

Patrick Martins Mendes

GOVERNANÇA DA SEGURANÇA: A Segurança da Informação alinhada aos Negócios

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Orientador:

Prof. Carlos Mendes, M.Sc., UFRJ, Brasil

Rio de Janeiro

2008

Patrick Martins Mendes

GOVERNANÇA DA SEGURANÇA: A Segurança da Informação alinhada aos Negócios

Monografia apresentada para obtenção do título de Especialista em Gerência de Redes de Computadores no Curso de Pós-Graduação Lato Sensu em Gerência de Redes de Computadores e Tecnologia Internet do Núcleo de Computação Eletrônica da Universidade Federal do Rio de Janeiro – NCE/UFRJ.

Aprovada em Dezembro de 2008.

Carlos Mendes

Prof. Carlos Mendes, M.Sc., UFRJ, Brasil

Dedico este projeto principalmente a DEUS, que me possibilitou superar todas as dificuldades encontradas, alcançando assim, meus objetivos; aos meus familiares, amigos e principalmente aos meus pais, que nos ajudaram nos momentos mais difíceis; e aos professores por todo apoio, sem o qual nada disto teria valor.

AGRADECIMENTOS

Agradeço primeiro a DEUS por nos ter capacitado e dado sabedoria e condições de fazer este trabalho, acreditando sempre nas promessas.

Aos meus pais e irmãos que, com amor e carinho me apoiaram em toda a jornada que seguimos e pela compreensão dos finais de semana que não pudemos comparecer.

Aos meus amigos por todo apoio e compreensão durante toda a execução desse projeto.

RESUMO

MENDES, Patrick Martins. **GOVERNANÇA DA SEGURANÇA: A Segurança da Informação alinhada aos Negócios**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

Este trabalho descreve um modelo que permitirá ao conselho administrativo a incorporação da Governança da Segurança da Informação como parte do seu processo de Governança Organizacional. A partir da utilização desse modelo, pretende-se que o conhecimento sobre os riscos relacionados à infra-estrutura de Tecnologia da Informação e Comunicação seja apresentado de forma objetiva ao conselho administrativo ao longo do planejamento estratégico.

O modelo apresentando foi elaborado tendo como base a estrutura de tomada de decisão utilizada pelos Sistemas de Informações Gerenciais. A seguir, foi proposta uma nova dimensão para contemplar: controles (o que), processos (como), pessoas (quem) e tecnologia (ferramentas automatizadas). Uma revisão de literatura sobre Governança de TI foi realizada para a identificação de modelos que pudessem oferecer alguma contribuição ao trabalho. O modelo COBIT e a norma ISO foram utilizados para definição dos objetivos de controle a serem implementados em cada nível e o modelo ITIL foi utilizado para definir os processos responsáveis pela implementação.

Algumas adaptações foram propostas para alguns processos do modelo ITIL para que o mesmo pudesse contemplar todos os objetivos de controle presentes na norma ISO e no modelo COBIT, todavia estas soluções apresentam-se como proposta de melhoria deste trabalho.

ABSTRACT

MENDES, Patrick Martins. **GOVERNANÇA DA SEGURANÇA: A Segurança da Informação alinhada aos Negócios**. Monografia (Especialização em Gerência de Redes e Tecnologia Internet). Núcleo de Computação Eletrônica, Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2008.

This work describes the development of a model thought to help the administration board of institutions to consider Information Security Governance as part of their global governance structure. The idea is to provide the proper knowledge about the risks posed by the Information Technology infrastructure in a pragmatic way, allowing for an efficient strategic planning.

The model is based on common, proven, decision making strategies used on Information Management Systems. A new dimension is added to those traditional Information Management Systems in order to accomplish: control (what), processes (how), people (who) and technology (automated tools). Through a study of some models of management and governance of Information Technology, the main body of the model was formed. COBIT and the ISO security standard were used to define the control objectives needed in each level.

The ITIL model was adapted to define the implementation of the processes, however these solutions have to be proposed for improvement of this work.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - Associação Brasileira de Normas Técnicas

BS - British Standard

CCSC - Commercial Computer Security Center

CEO - Chief Executive Officer

CMM - Capability Maturity Model for Software

COBIT - Control Objectives for Information and related Technology

CSO - Chief Security Officer

ERP - Enterprise Resource Planning

IEC - International Electrotechnical Commission

ISO - International Organization for Standardization

ITGI - IT Governance Institute

ITIL - Information Technology Infrastructure Library

ITSM - IT Service Management

NBR – Norma Brasileira

SIG - Sistemas de Informações Gerenciais

SIO - Sistemas de Informações Operacionais

SLA - Service Level Agreement

TI - Tecnologia da Informação

UK DTI - United Kingdom Department of Trade Center

SUMÁRIO

1 INTRODUÇÃO

A informação sempre esteve presente nas organizações e cumpria importante papel para a gestão do negócio, objetivando melhor produtividade, redução de custos, ganho de Market Share, aumento de agilidade, competitividade e apoio à tomada de decisão. Desta forma, a preocupação com a segurança destas informações já existiam. Na época em que as informações eram armazenadas em papel, a segurança era relativamente simples. Bastava trancar os documentos em algum lugar e restringir o acesso físico àquele local.

Com as mudanças tecnológicas e o uso de computadores de grande porte, a estrutura de segurança já ficou um pouco mais sofisticada, englobando controles lógicos, porém ainda centralizados.

Com a chegada dos computadores pessoais, das redes de computadores e do advento da internet que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que sem computadores, redes de comunicação e a internet, a prestação de serviços de informação pode ser tornar inviável.

Por esta razão, nos últimos anos as atividades relacionadas à Segurança das Informações passaram a ser uma rotina nas organizações. Mais do que ações tecnológicas, a Segurança passou a ser vista de uma forma mais abrangente, englobando preocupações como continuidade das operações, cultura dos funcionários e aspectos legais como SLA (Service Level Agreement) e monitoramento de funcionários. Um pouco dessas novas preocupações se devem a

eventos como os atentados de 11 de setembro nos EUA (Estados Unidos da América) assim como os escândalos contábeis das empresas WorldCom e Enron.

Este cenário ampliou a necessidade das organizações investirem mais em segurança, todavia para garantir os principais fatores da segurança da informação é necessário a implementação de vários controles de forma a reduzir as vulnerabilidades e conseqüentemente reduzir os riscos na qual uma organização está exposta.

Diante deste cenário, como é possível manter as informações seguras sem impactar nos processos de negócio da organização?

1.1 OBJETIVO

Este documento tem como objetivo apresentar uma metodologia de Governança da Segurança da Informação através do correlacionamento das metodologias COBIT e ITIL e da norma ISO 17799, que permitirá um melhor gerenciamento dos recursos e processos de TI, contribuirá para redução dos riscos inerentes ao uso da infra-estrutura de TI e permitirá a análise dos indicadores dos benefícios de se possuir uma infra-estrutura segura sem engessar os negócios da organização.

A partir da utilização desse estudo, pretende-se demonstrar que o conhecimento sobre os riscos relacionados à infra-estrutura de TI sejam apresentados de forma objetiva no momento da definição do planejamento estratégico.

A análise de riscos foi utilizada para a identificação dos riscos inerentes ao negócio, o modelo COBIT e a norma ISO 17799 foram utilizadas para definição dos

objetivos de controle a serem implementados e o modelo ITIL foi utilizado para definir os processos responsáveis pela implementação.

1.2 MOTIVAÇÃO

A motivação para o desenvolvimento deste documento surgiu a partir da identificação da grande dificuldade em direcionar os investimentos para a implementação de controles de segurança alinhada aos objetivos de negócio da organização, de forma a reduzir os riscos inerentes e garantir a segurança das informações.

As metodologias COBIT e ITIL e a norma ISO 17799 são ferramentas que atingiram um alto grau de maturidade e que possuem uma grande aceitação no mercado nacional e internacional, sendo um dos mais importantes fatores na definição das metodologias e normas que seriam utilizados na elaboração deste documento.

2 A INFORMAÇÃO E SUA IMPORTÂNCIA PARA OS NEGÓCIOS

De acordo com o Online Etymology Dictionary (2007), a palavra informação vem do Latim Informationem, cujo significado é compreendido como ***delinear, conceber idéia***. Segundo esta visão, o autor André L. N. Campos (2005) descreve que a informação é constituída a partir de um conjunto de dados que representam um ponto de vista evidenciando relações sobre eventos ou objetos. Portanto, a informação possui significado e causa impacto em menor ou maior grau, tornando-a elemento essencial da extração e criação do conhecimento.

Desta forma, pode-se afirmar que o conhecimento é a informação interpretada, ou seja, o conhecimento só poderá ser formado a partir da exposição do indivíduo à informação de modo que possa ser utilizada para importantes ações e tomadas de decisões.

Independente de segmento de mercado, do seu *Core Business* e porte, a informação sempre esteve presente nas organizações. Todas decidem suas estratégias de negócio, suas ações e seus planos com base em informações, seja ela uma análise de mercado, dados operacionais históricos e pesquisas. As informações são fundamentais e se revelam como um importante diferencial competitivo ligado ao crescimento e à continuidade do negócio através da geração do conhecimento.

Ainda segundo André L. N. Campos (2005), poderá até haver informação sem conhecimento, mas, não, conhecimento sem informação. A importância da informação é tamanha nos tempos atuais, que se diz, em nossa época, que vivemos na “Era da Informação”.

2.1 CRESCIMENTO DA DEPENDÊNCIA

Se realizarmos uma análise na forma como as empresas utilizavam a informação e administravam seus negócios, facilmente perceberemos uma profunda mudança nas ferramentas com o passar dos anos.

Inicialmente as empresas armazenavam suas informações em papel onde eram utilizadas técnicas de armazenamento e recuperação de informações de grandes arquivos. Esse método exigia um grande esforço para manter os dados atualizados bem como para recuperá-los, além de não possibilitarem a facilidade de cruzamento e análise dos dados.

Com a chegada dos primeiros computadores de grande porte, também conhecidos como Mainframe, as informações passaram a ser armazenadas de forma centralizada. Inicialmente esta promissora ferramenta possuía grandes limitações de armazenamento a preços elevados, fazendo com que muitas informações ainda fossem armazenadas em papéis.

Com o avanço da tecnologia, os Mainframes passaram a armazenar um volume maior de informações a preços mais acessíveis e se tornando a função central de processamento e armazenamento da organização. O acesso às informações era realizado a partir de milhares de terminais conectados diretamente ou através de uma rede.

Neste período, compartilhar informação passou a ser considerada uma prática moderna de gestão e necessária a empresas que buscam maior velocidade nas ações. Diante disto, com o surgimento das redes corporativas, tornou-se possível a interligação das diversas tecnologias de redes de computadores e a integração das mesmas com os mainframes e micro-computadores. A padronização

proposta pelas redes corporativas permitiu que os diversos computadores se comunicassem independentemente das suas arquiteturas de hardware e software, e conseqüentemente as informações passaram a ser mais digitalizadas e os processos mais automatizados.

Mais alguns anos e as empresas experimentam e aplicam, como nunca, a tecnologia da informação ao negócio. Os computadores tomam conta dos ambientes de escritório e quebram o paradigma de acesso local à informação e chegam a qualquer lugar do mundo através da rede mundial de computadores: a Internet.

Simultaneamente, a rede corporativa ganha performance e igualmente se pulveriza, passando a representar o principal canal de distribuição de informações internas e externas e de interligação de ambientes e processos, culminando com a integração dos parceiros da cadeia produtiva.

Logo surgem expressões e aplicações comerciais que se utilizam da moderna infra-estrutura de rede e computacional como *business-to-business*, *business-to-consumer*, *business-to-government*, *e-commerce*, *e-procurement*, e os sistemas integrados de gestão *ERP – Enterprise Resource Planning* que prometem melhor organização dos processos de negócio, e passam a representar um dos principais pilares de sustentação da empresa para alcançar o tão sonhado e promissor *digital marketplace*, onde os elementos da cadeia produtiva, como fornecedores, parceiros, clientes e governo passam a interagir também eletronicamente, integrando e compartilhando suas bases de conhecimento.

Esse panorama nos leva a perceber o alto grau de dependência que as empresas têm da informação – muito mais digitalizada, compartilhada e distribuída – além, conseqüentemente, de todos os elementos da infra-estrutura que a mantém.

Uma vez que a informação representa valor, e conseqüentemente contribui diretamente como um diferencial competitivo, é possível afirmar, que a informação é um bem, um ativo da organização e deve ser preservado e protegido tal quais os demais ativos da organização.

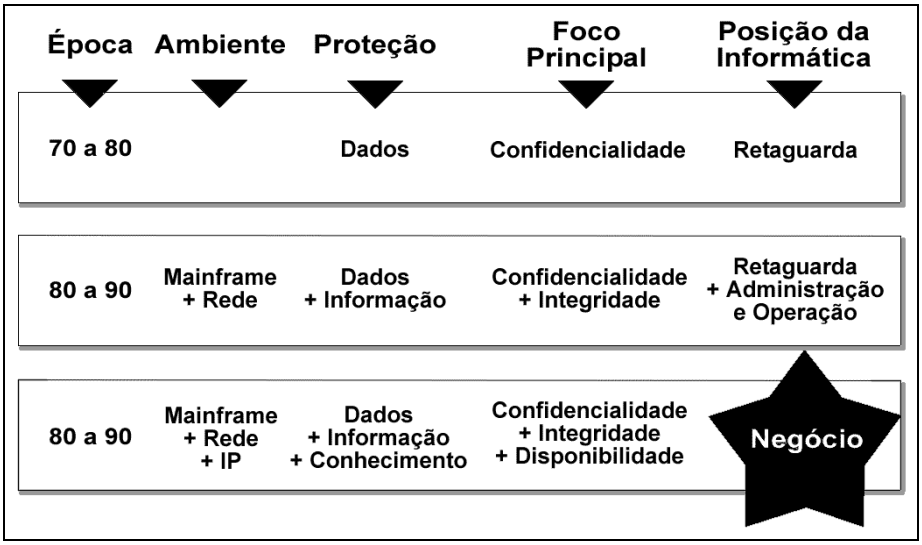

Figura 1: Evolução do cenário recente da segurança da informação

2.2 CONCEITOS GERAIS DA SEGURANÇA DA INFORMAÇÃO

Conforme visto, as organizações atualmente possuem um alto grau de dependência da informação, que representa valor e por isso deve ser protegida como todos os demais ativos.

Para que as informações possam ser protegidas de forma adequada, é necessário conhecer suas principais propriedades e identificar o seu ciclo de vida.

Toda informação possuem três propriedades que devem ser observadas, preservadas e protegidas para que esteja efetivamente sob controle: Confidencialidade, Integridade e Disponibilidade. Alguns autores denominam estas propriedades como pirâmide ou tríade da Segurança da Informação.

Confidencialidade: é a propriedade de que a informação não estará disponível ou divulgada a indivíduos, entidades ou processos sem autorização.

Integridade: A preservação da integridade envolve proteger as informações contra alterações em seu estado original, garantindo que as informações não sejam modificadas por pessoas não autorizadas.

Disponibilidade: é a garantia de que uma informação sempre poderá ser acessada, pelas pessoas e processos autorizados, independentemente do momento em que ela é requisitada e do local no qual está armazenada.

Podemos considerar como o ciclo de vida os momentos vividos pela informação e que podem colocá-la em risco. Segundo Marcos Sêmola (2003), os momentos em que as informações são expostas às ameaças e que as colocam em risco são justamente quando os ativos físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que mantém a operação da empresa. Estes momentos são conhecidos como **manuseio, armazenamento, transporte e descarte**.

Além de identificar as propriedades a serem protegidas é necessário conhecer do que é preciso se proteger para que possamos oferecer a segurança adequada. Para isto, é necessário analisar a interação de alguns agentes e considerarmos certos fatores: *Valor, Ameaça, Vulnerabilidade, Impacto, Risco.*

O diagrama a seguir nos apresenta de forma gráfica como todos os componentes vistos até o momento interagem entre si.

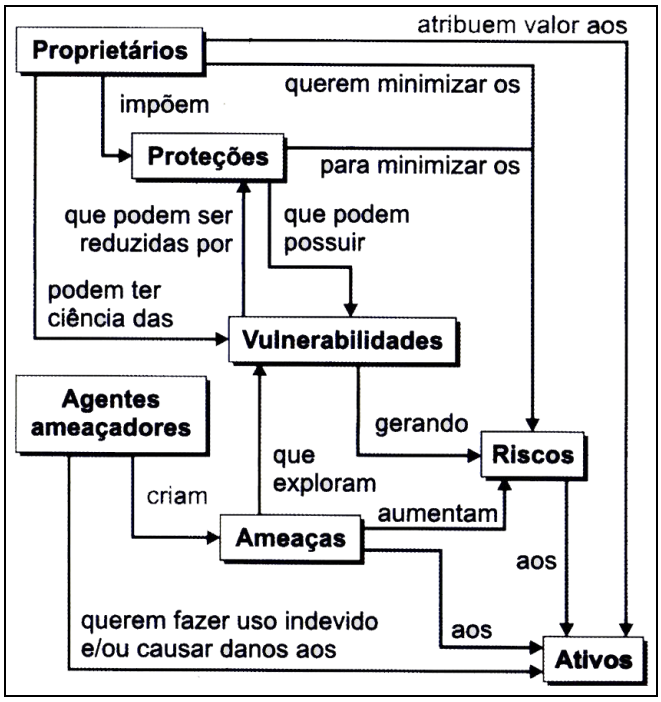

Figura 2: Interação entre os componentes básicos.

2.3 ANATOMIA DO PROBLEMA

Diante dos componentes apresentados podemos concluir que para qualquer iniciativa de solução de proteção é necessário identificar prioritariamente o problema com requinte de detalhes e segmentá-la de forma a permitir maior profundidade na análise de suas características.

Infelizmente muito executivos acreditam que o problema com a segurança da informação se resolve implementando apenas alguns controles tecnológicos como, por exemplo, a implementação de um firewall e um bom antivírus. Porém, atualmente a informação nas organizações transcende os aspectos tecnológicos, sendo alvos também por interferências provocadas por aspectos físicos e humanos. É fator crítico de sucesso para a anatomia do problema, que se identifiquem os elementos internos e externos que interferem nos riscos à segurança da informação.

Para que possamos conhecer exatamente quais são as vulnerabilidades existentes na organização, as ameaças que podem explorá-las, os riscos efetivos ao

qual a informação está exposta e os objetivos de negócios da organização que seriam impactados no caso de um incidente, de forma o prover soluções adequadas de proteção, é necessário a implementação de um processo de gestão de riscos.

2.4 COBIT

COBIT, do inglês, Control Objectives for Information and related Technology, é uma estrutura de relações e processos para dirigir e controlar o ambiente de TI para alcançar as metas da organização somando valor enquanto equilibra risco versus retorno sobre o investimento em TI e seus processos. Segundo Gustavo Alberto Alves (2006), TI passará a ter um papel de maior importância para o alcance das metas estipuladas pelos executivos, e não apenas como suporte à empresa.

O COBIT funciona como uma entidade de padronização que estabelece métodos formalizados para guiar a área de tecnologia das empresas, incluindo qualidade, níveis de maturidade e segurança da informação.

A estrutura do COBIT trata a tecnologia da informação em quatro domínios, para que possa refletir um modelo para os processos de TI. Esses domínios podem ser caracterizados pelos seus processos e pelas atividades executadas em cada fase de implementação da Governança Tecnológica. Os domínios do COBIT são: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoração e Avaliação.

O modelo COBIT define objetivos de controle, denominado High Level Objectives, como sendo declarações de um propósito ou resultado desejado a ser alcançado, por meio de implementação de controles em determinada atividade de TI. Quando atingidos, por meio da implementação eficaz dos respectivos controles, garantem o alinhamento da TI aos objetivos de negócio.

Para cada objetivo de controle, existe um conjunto de controles, que segundo o COBIT, são políticas, procedimentos, práticas e estruturas organizacionais, projetadas para prover razoável garantia de que os objetivos de negócio serão alcançados e que eventos indesejáveis serão prevenidos, ou apagados e corrigidos.

Além disto, para satisfazer os objetivos de negócio, as informações precisam estar em conformidade com os critérios de informação: Eficácia, Eficiência, Confidencialidade, Integridade, Disponibilidade, Conformidade, Confiabilidade, e com os recursos de TI: Pessoas, Aplicações, Infra-estrutura e Informações, destaca Gustavo.

O grau de importância de cada um dos critérios de informação é uma função do negócio e do ambiente em que a organização opera. Numa avaliação de riscos, esses critérios atribuem pesos diferentes aos Processos do COBIT, em função da importância no alcance dos respectivos Objetivos de Controle.

Como o COBIT foi desenvolvido para o gerenciamento dos processos de TI, um modelo de maturidade foi definido para cada um dos 34 objetivos de controle. Segundo o dicionário *Houaiss*, a maturidade significa o “estado, condição (de estrutura, forma, função ou organismo) num estágio adulto; condição de plenitude em arte, saber ou habilidade adquirida”, ou seja, é um estado de evolução contínuo conquistado ao longo de um período de existência. Desta forma, para que os gestores tenham uma visão real do seu cenário, é necessário medir o estado atual dos seus processos e para isso o COBIT segue o modelo do CMM (Capability Maturity Model for Software) que estabelece os seguintes níveis:

a) Nível 0 - Inexistente: Significa que o processo de gerenciamento não foi implementado;

b) Nível 1 - Inicial: O processo é realizado sem organização, de modo não planejado;

c) Nível 2 - Repetível: O processo é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido;

d) Nível 3 - Definido: O processo é realizado, documentado e comunicado na organização;

e) Nível 4 - Gerenciado: Existem métricas de desempenho das atividades, o processo é monitorado e constantemente avaliado;

f) Nível 5 - Otimizado: As melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos.

O resultado da avaliação do nível de maturidade (grau dos processos) ajuda a área de TI a identificar o grau atual e como evoluir para melhorar os processos da organização, permitindo a evolução desses. O nível ótimo correspondente é determinado individualmente, de acordo com a natureza da instituição, ameaças e oportunidades viabilizadas por TI. Além disto, o COBIT fornece orientações, específicas para cada processo, do que deve ser trabalhado para atingir determinado nível de maturidade.

2.5 ITIL

Atualmente a TI possui um papel de grande importância nas organizações, atuando não apenas como suporte, mas participando efetivamente para o alcance dos seus objetivos de negócios. Por esta razão, o controle do ambiente de TI tem se tornado um item de extrema importância e alta complexidade, sendo necessária a implementação de uma metodologia de gestão, de modo a refletir verdadeiramente as atividades e responsabilidades da TI.

O ITIL-ITSM fornece essa metodologia com uma plataforma focada nos processos e nas suas relações de dependência. O ITIL fornece uma orientação para a TI baseada nas melhores práticas e num ambiente de qualidade, envolvendo pessoas, processos e tecnologia para dirigir a TI como um negócio.

O ITIL é um conjunto de livros que busca promover a gestão com foco no cliente e na qualidade dos serviços de TI. O ITIL endereça estruturas de processos para a gestão de uma organização de TI apresentando um conjunto compreensivo de processos e procedimentos gerenciais organizados em disciplinas com os quais uma organização pode fazer sua gestão tática e operacional em vista de alcançar o alinhamento estratégico com os negócios.

Atualmente o ITIL tornou-se uma referência para a Gestão e Serviços, sendo adotado globalmente. O uso efetivo das melhores práticas definidas na ITIL traz inúmeros benefícios às organizações, tais como: melhoria na utilização dos recursos, maior competitividade, redução de retrabalhos, eliminação de trabalhos redundantes, melhoria da disponibilidade etc..

O princípio básico da biblioteca ITIL é o objeto de seu gerenciamento: a infra-estrutura de TI. O ITIL descreve os processos que são necessários para dar suporte à utilização e ao gerenciamento da infra-estrutura de TI. Outro princípio fundamental do ITIL é o fornecimento de qualidade de serviço aos clientes de TI com custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia e como estes trazem valor estratégico ao negócio. Através de processos padronizados de gerenciamento do ambiente de TI é possível obter uma relação adequada entre custos e níveis de serviço prestados pela área de TI.

O ITIL consiste de um conjunto de melhores práticas que são inter-relacionadas para minimizar o custo, ao mesmo tempo em que aumenta a qualidade dos serviços de TI entregues aos usuários. O ITIL é organizado em 5 módulos principais: *Perspectiva de Negócios, Gerenciamento de Aplicações, Entrega de Serviços, Suporte a Serviços, Gerenciamento de Infra-estrutura.*

Embora o modelo ITIL não tenha um módulo dedicado ao Gerenciamento de Segurança Computacional, ele faz referência a este tema apontando em um documento como o mesmo poderia ser incorporado através dos processos descritos nos módulos de Suporte a Serviços e Entrega de Serviços.

Ao usar o ITIL, a organização se torna capaz de melhorar a qualidade, eficiência e eficácia na prestação de serviços, além de diminuir a exposição ao risco operacional. Os processos ITIL precisam ser implementados para cada organização, pois correspondem a um modelo e não uma regra rígida a ser seguida.

Apesar do modelo ITIL possuir processos bem definidos para auxiliar na Governança da Tecnologia da Informação, neste trabalho identifica-se a necessidade de algumas adaptações para que ele possa ser utilizado para implementar todos os requisitos de um modelo de Governança da Segurança da Informação. Essas adaptações estão relacionadas principalmente com a forma de como tratar incidentes de segurança computacional.

2.6 NORMA NBR ISO/IEC 17799

Diante do cenário atual, onde a informação exerce um importante papel nas organizações, gerando conhecimento e apoiando os executivos na tomada de decisão, sendo, desta forma essencial para os negócios, verifica-se a necessidade garantir a sua segurança.

Independente da forma no qual a informação está representada é sempre recomendado que ela seja protegida adequadamente. Com isso, a segurança da informação é a proteção da informação das ameaças na busca de manter a continuidade do negócio, diminuir os riscos e maximizar retornos.

Diante dessa necessidade, o governo britânico através do UK DTI (Department of Trade Center) criou, em 1987, o CCSC (Commercial Computer Security Center), cujo objetivo era a criação de critérios para a avaliação da segurança e de um código de segurança para os usuários das informações, de uma forma geral. No ano de 1989 foi publicada a primeira versão do código de segurança, que na época foi denominado de PD0003 - Código de Gerenciamento de Segurança da Informação.

Em 1995 esse código foi revisado, ampliado e publicado como uma norma britânica (BS), a BS7799-1:1995 (Information Technology - Code of practice for information security management) e em 1998 foi publicada a segunda parte dessa norma reconhecida como BS7799-2:1998 (Information Security Management Systems).

A BS7799-1:1995 é a parte da norma que é planejada como um documento de referência das boas práticas de segurança na organização e a BS7799-2:1998 é a parte da norma que tem o objetivo de estabelecer um modelo de gestão da segurança na organização.

Após um árduo trabalho de internacionalização, a BS 7799 foi reconhecida pelos países membros da ISO (International Organization for Standardization), em dezembro de 2000, e homologada como ISO/IEC 17799:2000.

Em dezembro de 2000 a ABNT (Associação Brasileira de Normas Técnicas) reconheceu a norma ISO como um padrão brasileiro, sendo publicada como NBR ISO/IEC 17799 – Código de Prática para a Gestão da Segurança da Informação (2001).

A norma de Segurança da Informação trouxe não apenas vários controles de segurança, mas permitiu a criação de um mecanismo de certificação das organizações, semelhante às certificações ISO já existentes, contudo esta nova certificação "afirma" que a organização certificada manipula os seus dados e os dados dos clientes de forma segura, independentemente da forma como eles estão armazenados. Em 2005 a norma sofreu uma revisão e foi publicada sua nova versão, a NBR ISO/IEC 17799:2005, que cancela e substitui a edição anterior.

A norma nacional de segurança de informação é dividida nos 10 macros controles: Política de Segurança, Segurança Organizacional, Classificação e Controle dos Ativos da Informação, Segurança em Pessoas, Segurança Física e do Ambiente, Gerenciamento de Operações e Comunicações, Controle de Acesso, Desenvolvimento da Segurança de Sistemas, Gestão da Continuidade do Negócio, Conformidade.

Cada um destes controles é subdividido em vários outros controles, num total de 137 controles de segurança. Os Controles da norma nacional de segurança visam manter e gerir a segurança da informação nas organizações. Atualmente no Brasil, a NBR ISO/IEC 17799 é considerada a principal referência para o processo de gestão da segurança da informação nas organizações.

3 MODELO PARA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

3.1 GOVERNANÇA DE TECNOLOGIA DA INFORMAÇÃO

No capitulo anterior verificou-se a importância das informações para as decisões estratégicas das organizações que, por esta razão, necessitam ser adequadamente gerenciadas e protegidas.

Além disto, com o avanço das tecnologias, verificou-se como os sistemas e os serviços de TI desempenham importante papel no ciclo de vida da informação, sendo indispensável à execução do negócio das organizações. Diante deste cenário surgiu o conceito de Governança Tecnológica, do termo inglês *IT Governance*, no qual se busca um alinhamento de TI com os objetivos da organização.

A governança envolve direcionamento de TI e controle da Gestão, verificação do retorno do investimento e do controle dos riscos, análise do desempenho e das mudanças na TI, e alinhamento com as demandas futuras da atividade fim - foco interno - e com a atividade fim de seus clientes - foco externo. Essa abrangência é ilustrada na Figura 3. A gestão preocupa-se com o planejamento, a organização, a implementação, a implantação e a manutenção da infra-estrutura de TI, e com o gerenciamento dos processos com foco no suporte e no fornecimento dos serviços.

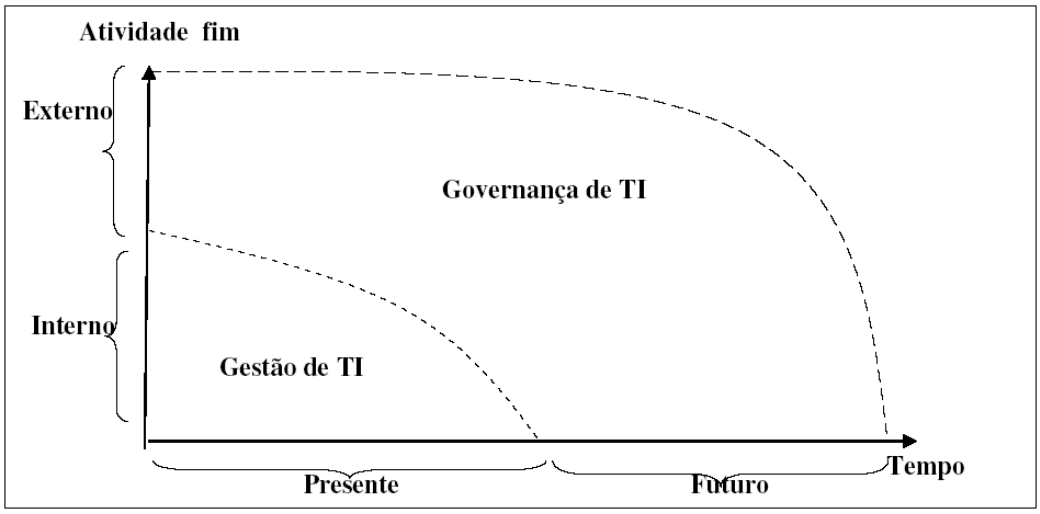

Figura 3: Abrangência da Governança e da Gestão de TI

3.2 GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

Uma vez que a informação é vital para as organizações e, por isso, precisam ser protegidas verifica-se a necessidade e importância de se alcançar um modelo de Governança da Segurança da Informação como um subconjunto da Governança de TI e, conseqüentemente, da Governança Organizacional.

Segundo o ITGI – IT Governance Institute, a Governança da Segurança da Informação é responsabilidade dos Diretores e dos Executivos Seniores, sendo parte integrante e transparente da Governança Corporativa e alinhada com a Governança de TI.

Desta forma, o modelo de Governança da Segurança da Informação permitirá que as organizações não tratem a Segurança Computacional apenas no âmbito tecnológico, mas reconhecida como parte integrante do planejamento estratégico das organizações no processo de tomada de decisão.

Todavia, atualmente a responsabilidade sobre segurança computacional é delegada ao gerente de segurança, também conhecido como CSO (*Chief Security Officer*) das organizações, gerando conflitos em relação ao orçamento destinado a

esta área e a necessidade de impor medidas que vão além de seu escopo de atuação. Diante deste cenário, é comum encontrar organizações onde as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo como conseqüência a falta de recursos para minimizar os riscos existentes ao nível exigido pela estratégia organizacional.

Segundo um relatório divulgado pelo Corporate Governance Task Force, é proposto que para proteger melhor a infra-estrutura de TI é necessário que as questões relacionadas à segurança da informação sejam incorporadas às ações de governança das organizações.

A adoção deste modelo permite quebrar o paradigma estabelecido na área de TI, que ainda é vista como uma área de custos para a grande maioria das empresas do que como um diferencial competitivo, permitindo que TI seja alinhada com as estratégias da organização, permitindo que a segurança da informação deixe de ser tratada apenas como uma questão técnica, passando a ser um desafio estratégico e administrativo, como parte integrante das “melhores práticas corporativas”, não deixando de cobrir aspectos relacionados com as pessoas, processos e tecnologia.

Para atender a estes requisitos, será realizado o correlacionamento dos modelos COBIT, ITIL e ISO 17799. Esses modelos são utilizados amplamente no mundo, porém de forma isolada. O grande diferencial deste trabalho está na combinação do que cada modelo possui de melhor, criando uma solução customizada, que seja capaz de atender às demandas de negócio de cada organização.

3.3 REQUISITOS PARA UM MODELO DE GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

No cenário organizacional encontramos empresas de diversos segmentos, portes e apresentando diferentes necessidades. Por esta razão, é necessário que seja definido um conjunto de requisitos universais capaz de atender a todas estas organizações, a fim de estabelecer um modelo de governança da segurança da informação.

De forma a estabelecer um modelo de governança da segurança da informação capaz de atender a empresas de diferentes portes, segmentos e com necessidades distintas, um conjunto de requisitos deve ser definido para direcionar os mais diversos esforços.

Diante desta necessidade, o Corporate Governance Task Force (2008) definiu um conjunto de requisitos reconhecidos pelo mercado e identificados tanto na normativa de segurança, como a ISO 17799, FISMA (Federal Information Security Management Act) etc., como na política de segurança das empresas de grande porte, capaz de abranger procedimentos associados à segurança da informação.

Os requisitos definidos pelo Corporate Governance Task Force são:

1. Os CEOs (Chief Executive Officers) precisam de procedimentos para conduzir uma avaliação periódica sobre segurança da informação, revisar os resultados com sua equipe e comunicar o resultado para o conselho administrativo;

2. Os CEOs precisam adotar e patrocinar boas práticas corporativas para segurança computacional, sendo municiados com indicadores objetivos que os façam considerar a área de segurança computacional como um importante centro de investimentos na organização, e não apenas um centro de despesas;

3. Organizações devem conduzir periodicamente uma avaliação de risco relacionada à informação como parte do programa de gerenciamento de riscos;

4. Organizações precisam desenvolver e adotar políticas e procedimentos baseados na análise de risco para garantir a segurança da informação;

5. Organizações precisam estabelecer uma estrutura de gerenciamento da segurança da informação para definir explicitamente o que se espera de cada indivíduo (papéis e responsabilidades);

6. Organizações precisam desenvolver planejamento estratégico e iniciar ações para prover a segurança adequada para a rede de comunicação, os sistemas e a informação;

7. Organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas;

8. Organizações precisam divulgar as informações sobre segurança computacional, treinando e educando os indivíduos;

9. Organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados à segurança da informação;

10. Organizações precisam criar e executar um plano para remediar vulnerabilidades ou deficiências que comprometam a segurança da informação;

11. Organizações precisam desenvolver e colocar em prática procedimentos de resposta a incidentes;

12. Organizações precisam estabelecer planos, procedimentos e testes para prover a continuidade das operações;

13. Organizações precisam usar as melhores práticas relacionadas à segurança computacional, como a ISO 17799, para medir o nível alcançado em relação à segurança da informação.

Após a definição dos requisitos, realizaremos o correlacionamento com a estrutura de tomada de decisão gerenciais em seus três níveis, operacional, tático e estratégico, de forma a permitir a evolução dos dados (nível operacional) em informações (nível tático) e posteriormente em conhecimento (nível estratégico) para prover o conhecimento necessário aos gestores para o planejamento estratégico das organizações.

Apesar da importância e da necessidade dos requisitos apresentados, uma vez que estes orientam os gestores a direcionar os mais diversos esforços, o ponto mais importante proposto neste trabalho está na forma como estes requisitos são correlacionados e em quais níveis de gerenciamento os mesmos devem ser incluídos.

Para isto, será realizada uma combinação dos principais modelos COBIT e ITIL e da norma ISO 17799. Estes modelos vêm sendo utilizados largamente em organizações de todo o mundo nos últimos anos, todavia de forma isolada. Estes modelos representam as melhores práticas desenvolvidas, testadas e aprovadas por especialistas.

Nas seções seguintes será apresentado o correlacionamento dos requisitos necessários para a definição de um modelo de governança da segurança da informação com os modelos COBIT e ITIL e a norma ISO 17799.

3.4 RELAÇÃO DOS PROCESSOS ENTRE OS MODELOS COBIT, ITIL E A NORMA ISO 17799

Para consubstanciar o uso integrado do modelo COBIT, do modelo ITIL e da norma ISO 17799 em um Modelo de Governança da Segurança da Informação, apresenta-se na Tabela 1 uma correlação entre os objetivos de controle do COBIT e

os apresentados na norma ISO 17799 e os processos descritos no modelo ITIL (Suporte a Serviços e Entrega de Serviços).

A tabela a seguir apresenta o mapeamento realizado entre estes modelos e a estruturação dos objetivos de controles nos níveis Estratégico, Tático e Operacional.

Tabela 1: Relacionamento de Processos entre os Modelos ITIL, COBIT e a norma ISO 17799.

	Objetivos de Controle do COBIT	Objetivos de Controle do COBIT referenciados na ISO 17799	Objetivos de Controle do COBIT referenciados no modelo ITIL
Nível Estratégico	PO – Planejamento e Organização		
	PO1 – Definir o Plano Estratégico de TI	N/A	N/A
	PO2 – Definir a Arquitetura da Informação	A	N/A
	PO3 – Determinar o Direcionamento Tecnológico	A	N/A
	PO4 – Definir os Processos de TI, Organização e Relacionamentos	A	A
	PO5 – Gerenciar o Investimento em TI	A	A
	PO6 – Comunicar os Objetivos Gerenciais e Direcionamento	A	N/A
	PO7 – Gerenciar Recursos Humanos	A	N/A
	PO8 – Gerenciar Qualidade	A	N/A
	PO9 – Avaliar e Gerenciar Riscos de TI	A	N/A
	PO10 – Gerenciar Projetos	N/A	A
Nível Operacional e Nível Tático	AI – Aquisição e Implementação		
	AI1 – Identificar Soluções Automatizadas	A	A
	AI2 – Aquisição e Manutenção de Software	A	N/A
	AI3 – Adquirir e Manter Infra-estrutura Tecnológica	A	A
	AI4 – Permitir Operação e Uso	A	A
	A15 – Obter Recursos de Tecnologia da Informação	A	N/A
	AI6 – Gerenciar Mudanças	A	C
	AI7 – Instalar e Autorizar Soluções e Mudanças	A	A
	DS – Entrega e Suporte		
	DS1 – Definir e Gerenciar Níveis de Serviço	A	C
	DS2 – Gerenciar Serviços de Terceiros	A	C
	DS3 – Gerenciar Desempenho e Capacidade	A	C
	DS4 – Garantir a Continuidade do Serviço	A	C
	DS5 – Garantir a Segurança do Sistema	C	C
	DS6 – Identificar e Alocar Custos	N/A	C
	DS7 – Educar e Treinar Usuários	A	N/A
	DS8 – Gerenciar Central de Serviços e Incidentes	A	C

	Objetivos de Controle do COBIT	Objetivos de Controle do COBIT referenciados na ISO 17799	Objetivos de Controle do COBIT referenciados no modelo ITIL
	DS9 – Gerenciar Configuração	A	C
	DS10 – Gerenciar Problemas	A	A
	DS11 – Gerenciar Dados	A	N/A
	DS12 – Gerenciar Ambiente Físico	A	A
	DS13 – Gerenciar Operações	A	N/A
Nível Estratégico	ME – Monitoramento e Avaliação		
	ME1 – Monitorar e Avaliar o Desempenho de TI	A	N/A
	ME2 – Monitorar e Avaliar o Controle Interno Interno	A	N/A
	ME3 – Garantir Conformidade com a Legislação	A	N/A
	ME4 – Prover Governança de TI	A	N/A

Paro o relacionamento realizado na Tabela 1 foram utilizados os modelos COBIT 4.0, ITIL e a norma ISO 17799:2005, onde foram categorizados em 3 níveis:

- N/A – Não há relacionamento;
- A – Alguns aspectos dos objetivos de controle são endereçados, porém os requisitos não são completos;
- C – Os requisitos dos objetivos de controles são completamente atendidos.

Ao analisarmos a tabela, verificamos que o modelo ITIL descreve de forma detalhada um conjunto de boas práticas para os processos relativos ao Suporte e a Entrega de Serviços (domínio DS), porém não cobre todos os requisitos de controle relacionados ao gerenciamento de TI, se compararmos ao COBIT.

Alguns objetivos de controle do domínio Planejamento e Organização (PO) do COBIT são tratados superficialmente através dos processos definidos no ITIL. Além disto, o domínio Monitoramento e Avaliação (ME) do COBIT não é abordado pelo ITIL.

Além disto, os processos do ITIL estão estruturados e detalhados para indicar como devem ser implementados e quem devem implementá-los (papéis e responsabilidades), não focando o que deve ser abordado no gerenciamento de TI.

3.5 IDENTIFICAÇÃO DE REQUISITOS DE SEGURANÇA A PARTIR DE UMA ANÁLISE DE RISCO

Um modelo de Governança de Segurança da Informação deverá prover mecanismos para a identificação dos requisitos de segurança adequados a uma organização. A ISO/IEC 17799:2005 aponta três fontes principais para essa identificação:

- Através da análise de risco dos ativos da organização são identificadas as ameaças aos ativos, as vulnerabilidades e suas respectivas probabilidades de ocorrência são avaliadas, bem como o impacto potencial é estimado;
- A legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros, contratados e prestadores de serviço têm que atender;
- O conjunto particular de princípios, objetivos e requisitos para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os gastos com os requisitos de controles necessitam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas na segurança. As técnicas de avaliação de risco podem ser aplicadas em toda a organização ou apenas em parte dela, assim como

em um sistema de informação individual, componentes de um sistema específico ou serviços, quando for viável, prático e útil.

A avaliação de risco é uma consideração sistemática a respeito de seguinte:

- Do impacto nos negócios como resultado de uma falha de segurança, levando-se em conta as potenciais conseqüências da perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos;
- Da probabilidade de tal falha realmente ocorrer à luz das ameaças e vulnerabilidades mais freqüentes e nos controles atualmente implementados.

Os resultados da avaliação de risco ajudarão a direcionar e determinar ações gerenciais e prioridades mais adequadas para um gerenciamento dos riscos da segurança da informação e a selecionar os objetivos de controles a serem implementados para a proteção contra esses riscos.

É necessário realizar análises críticas periódicas dos riscos de segurança e dos controles implementados para o seguinte fim:

- Considerar as mudanças nos requisitos de negócio e suas prioridades;
- Considerar novas ameaças e vulnerabilidades;
- Confirmar que os controles permanecem eficientes e adequados.

Convém que as análises críticas sejam executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações de risco feitas anteriormente e das mudanças nos níveis de riscos que a direção considera aceitável para os negócios. As avaliações de risco são sempre realizadas em nível

amplo primeiramente, como uma forma de priorizar recursos em áreas de alto risco, e então em um nível mais detalhado, para solucionar riscos específicos.

Para a identificação dos requisitos de segurança de uma organização, neste trabalho propõe-se a utilização das avaliações e diagnósticos apresentados pelo modelo COBIT.

3.6 ESTRUTURA DE DECISÃO DE SISTEMAS DE INFORMAÇÃO GERENCIAIS

Segundo Sérgio Rodrigues Bio (1994), os sistemas de informação são classificados em dois grupos:

- Sistemas de Apoio às operações, conhecidos como sistemas de informações Operacionais (SIOs);
- Sistemas de Apoio à gestão, conhecidos como Sistemas de Informações Gerenciais (SIGs).

Os sistemas de informações operacionais são sistemas processadores de transações, ou seja, sistemas que servem para o processamento de transações rotineiras. Os sistemas de informações gerenciais (SIGs), que é o alvo deste trabalho, são sistemas utilizados para auxiliar os gestores no processo decisório.

Um SIG é definido como um sistema para coleta, armazenamento, recuperação e processamento de informações, de forma a torná-las em conhecimento que serão utilizadas pelo gestor na sua tomada de decisão.

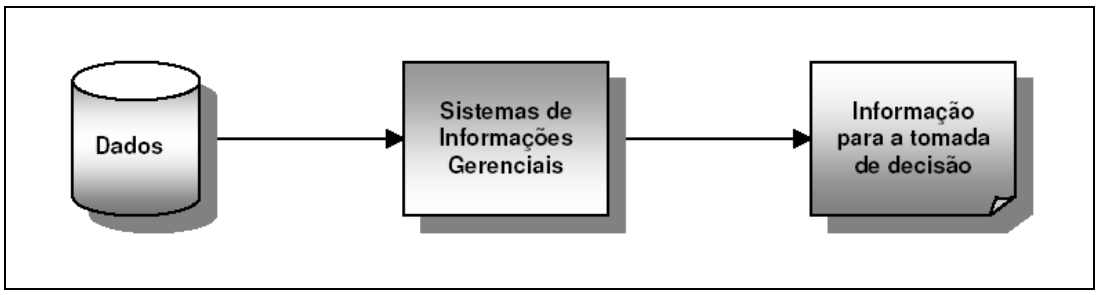

Figura 4: Representação simplificada para Sistemas de Informações Gerenciais

Segundo Djalma de Pinho Rebouças de Oliveira (1998), uma decisão pode ser definida como “a escolha entre vários caminhos alternativos que levam a um determinado resultado”, acrescentando como elemento básico que, para “um adequado processo decisório é necessário ter um sistema de informação eficiente”.

Uma forma de associar a informação à tomada de decisão pode ser representada graficamente, conforme a Figura 5.

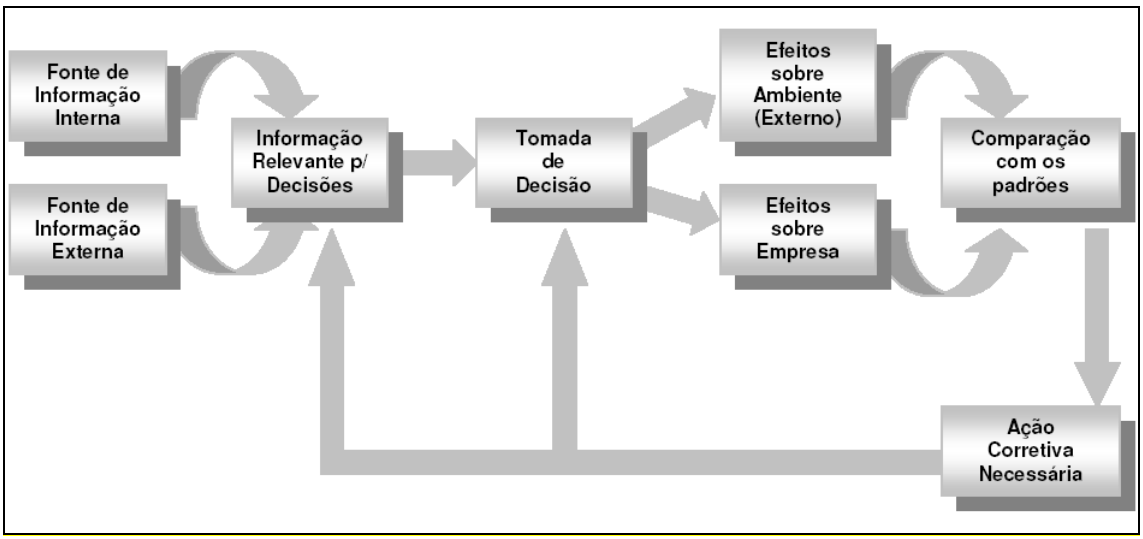

Figura 5: Interação da Informação com o Processo Decisório

A concepção de um sistema de informações que auxilie o gestor a melhorar suas decisões não depende apenas da identificação dos modelos decisórios dos gestores e de suas necessidades informativas. Muitas vezes, faz-se necessário repensar o próprio modelo de decisão, alem de utilizar informação adicional para

determinar a probabilidade de ocorrência de cada estado da natureza, a fim de reduzir o problema da incerteza.

O modelo de informações empresarial relaciona as informações com a sinergia necessária para gestão dos negócios e das funções empresariais. As informações são estruturadas nos níveis operacional, gerencial e estratégico, visando atender todos os requisitos funcionais estabelecidos e necessários. Cada função empresarial pode ser desmembrada ou decomposta em seus respectivos módulos. Nesse caso, conforme apresentado na Figura 6, a ênfase não está na ação e sim nas informações necessárias, relatando as informações estratégicas, relacionada no nível macro com o meio ambiente interno e externo, as informações gerenciais ou táticas – agrupadas, sintetizadas, totais, percentuais, acumuladas, plurais etc. e as informações operacionais – do dia-a-dia, pontuais.

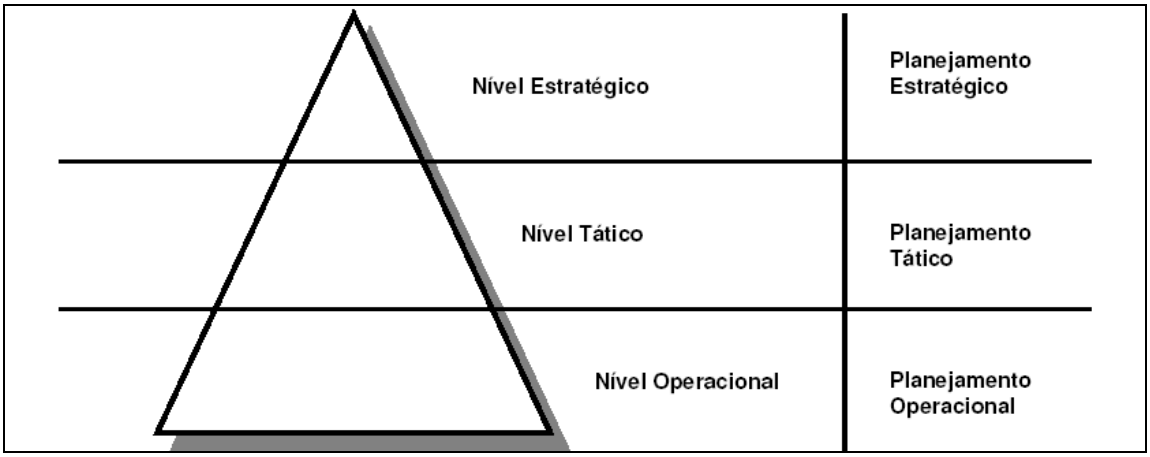

Figura 6: Os tipos de planejamento nas empresas

Com o apoio de uma base de dados unificada, as estruturas empresariais e respectivos níveis hierárquicos passarão a ser mais dinâmicos, eliminando barreiras e divisões que separem a alta administração do corpo gestor e do corpo técnico, provendo maior integração e envolvimento de todos, preferencialmente focados no negócio da empresa.

Além dos procedimentos e processos de seleção e organização das informações para sua efetiva utilização, os gestores deveriam ter sistemas de informações efetivos, que processem o grande volume de dados gerados e produzam informações e conhecimentos válidos, úteis, de boa qualidade e oportunos para os negócios da organização.

As informações e o conhecimento gerados a partir dos dados históricos da empresa propiciarão a identificação de problemas e necessidades nos níveis estratégicos, tático e operacional, bem como poderão fornecer subsídios para avaliar o impacto das diversas decisões a serem tomadas.

Para a definição de um modelo de Governança da Segurança da informação será estabelecida uma estrutura baseada nos modelos de tomada de decisão em Sistemas de Informações Gerenciais, de forma a garantir a constante avaliação dos objetivos, desafios, metas, estratégias e projetos.

A estrutura de tomada de decisão é dividida em 3 níveis: nível estratégico, nível tático e nível operacional.

Nível Estratégico: Neste nível os controles estratégicos decorrem do processo de planejamento estratégico e envolve as relações das empresas com o ambiente controlando o desempenho empresarial como um todo. Neste nível é gerado conhecimento macro, objetivo e relacionado a todo o ambiente interno e externo.

Nível Tático: No nível tático, os padrões de controle e avaliação são estabelecidos a partir de objetivos departamentais para avaliar os resultados de cada área e dos sistemas administrativos. O foco do controle tático é o resultado global da área, mediante visão integrada de todas as operações.

Nível operacional: No nível operacional, o controle e a avaliação são realizados pela execução das operações, ou seja, sobre a própria execução das tarefas. Neste nível são gerados dados do dia-a-dia, pontuais etc.

Diante desta estrutura, para realizar o processo de extração do conhecimento necessário ao gestor para o planejamento estratégico da organização é necessária a implementação de um sistema capaz de armazenar os mais diversos tipos de dados relacionados à segurança computacional provenientes do ambiente, conhecido como Data Warehouse.

Uma vez implementado o Data Warehouse, o sistema será alimentado com dados como matéria prima bruta. Através dos processos do modelo ITIL, o sistema de informação permitirá que esses dados sejam coletados e armazenados (nível operacional) e a seguir, trabalhados para que possam gerar informações no nível tático. Em seguida, as informações serão estruturadas em conhecimento (nível gerencial) a partir dos processos do modelo COBIT e das técnicas de extração de conhecimento das bases de dados.

Para agregar maior valor ao conhecimento gerado, propõe-se a estruturação dos requisitos propostos na seção 3.3 de uma forma que seja possível dar enfoque em controles, processos, pessoas e tecnologias, compondo uma matriz 3x4, que está representada através da Figura 7.

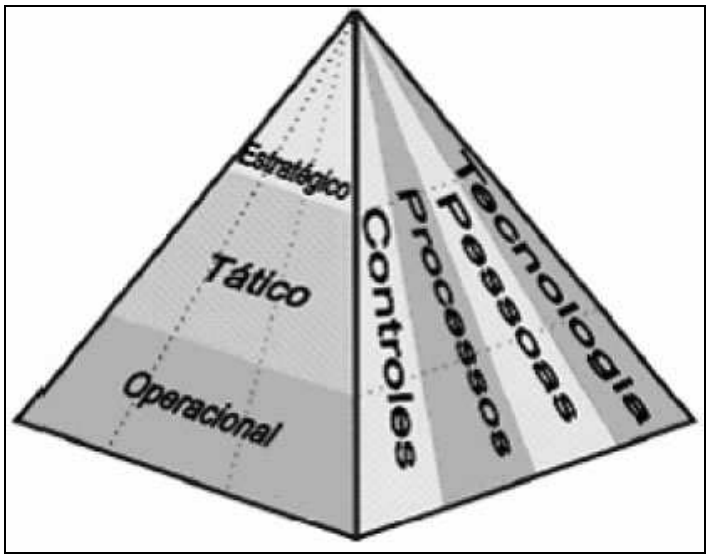

Figura 7: Estrutura proposta na análise correlacional

A definição do que será abordado em cada um dos itens da primeira dimensão (controles, processos, pessoas e tecnologia) é:

a) **Controles (o que):** Relação dos objetivos de controle a serem aplicados;

b) **Processos (como):** Descrição dos processos necessários para implementação dos objetivos de controle;

c) **Pessoas (quem):** Papéis e responsabilidades dos indivíduos envolvidos com os processos e objetivos de controle definidos;

d) **Tecnologia (ferramentas):** Identificação das ferramentas automatizadas de apoio à implementação dos processos e do sistema de informação gerencial.

Na segunda dimensão, onde são abordados os níveis da estrutura de tomada de decisão (operacional, tático e estratégico), refere-se a:

a) **Operacional:** Atividades necessárias para manter a infra-estrutura de TI em funcionamento;

b) **Tático:** Atividade pro ativas com revisões periódicas, busca contínua pela qualidade e possibilidade de planejamento em longo prazo;

c) **Estratégico:** Gerar conhecimento para permitir a visão organizacional para as questões de segurança computacional a partir de avaliações, auditorias, definição de níveis de maturidade dos objetivos de controle definidos e processos de extração de conhecimento de base de dados.

A seguir, é apresentada uma tabela contendo os requisitos definidos na sessão 3.3 relacionados às estratégias para a implementação e as estratégias para a implementação utilizando os modelos COBIT e ITIL e a norma ISO 17799.

Tabela 2: Proposta de estratégia para implementação dos requisitos identificados

Requisitos mapeados	Estratégia para a Implementação
1. Os CEOs (Chief Executive Officers) precisam ter um mecanismo para conduzir uma avaliação periódica sobre segurança da informação, revisar os resultados com sua equipe e comunicar o resultado para a mesa diretora.	Modelo COBIT
2. CEOs precisam adotar e patrocinar boas práticas corporativas para segurança computacional, sendo municiados com indicadores objetivos que os façam considerar a área de segurança computacional como um importante centro de investimentos na organização, e não apenas um centro de despesas.	Modelo COBIT e Modelo ITIL
3. Organizações devem conduzir periodicamente uma avaliação de risco relacionada à informação como parte do programa de gerenciamento de riscos.	Modelo COBIT e Análise de Risco
4. Organizações precisam desenvolver e adotar políticas e procedimentos baseados na análise de risco para garantir a segurança da informação.	Modelo COBIT e norma ISO 17799
5. Organizações precisam estabelecer uma estrutura de gerenciamento da segurança para definir explicitamente o que se espera de cada indivíduo (papéis e responsabilidades).	Modelo ITIL expandido
6. Organizações precisam desenvolver planos e iniciar ações para prover a segurança adequada para a rede de comunicação, os sistemas e a informação.	Modelo ITIL (gerência de continuidade)
7. Organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas.	Modelo COBIT e Modelo ITIL
8. Organizações precisam divulgar as informações sobre segurança computacional, treinando e educando os indivíduos.	Modelo ITIL expandido
9. Organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados à segurança da informação.	Modelo COBIT e modelo ITIL
10. Organizações precisam criar e executar um plano para remediar vulnerabilidades ou deficiências que comprometam a segurança da informação.	Modelo ITIL expandido
11. Organizações precisam desenvolver e colocar em prática procedimentos de resposta a incidentes.	Modelo ITIL expandido
12. Organizações precisam estabelecer planos, procedimentos e testes para prover a continuidade das operações.	Modelo COBIT e Modelo ITIL

Requisitos mapeados	Estratégia para a Implementação
13. Organizações precisam usar as melhores práticas relacionadas à segurança computacional para medir a performance da segurança da informação.	Modelo COBIT, Modelo ITIL e norma ISO 17799

Através de uma correlação dos objetivos de controle presentes no modelo COBIT e na norma ISO 17799 com os processos descritos no modelo ITIL, neste trabalho identificou-se que os módulos de Suporte a Serviços e Entrega de Serviços do modelo ITIL não estão estruturados para implementar todos os objetivos de controle apresentados para o nível Operacional e Tático.

Para que o modelo ITIL seja capaz de implementar todos os objetivos de controle apresentados pela norma ISO 17799 e pelo modelo COBIT para os níveis operacional e tático, deve-se realizar a adaptação dos processos ITIL de ‘Gerenciamento de Incidentes’, ‘Gerenciamento de Problemas’ e ‘Gerenciamento de Mudanças’ (reconhecido na Tabela 2 como ITIL Adaptado) para que esses processos permitam a reação aos incidentes de segurança computacional no nível operacional, além dada inserção de um novo processo de ‘Gerenciamento de Comportamento’ (reconhecido na Tabela 2 como ITIL Estendido), a ser utilizado no nível tático. Todavia, estas adaptações não fazem parte do escopo deste trabalho e apresenta-se como uma proposta de melhoria.

A seguir, a Tabela 3 apresenta o relacionamento das estratégias de implementação identificadas na (Tabela 2) com a estrutura de decisão de sistemas de informação gerenciais em suas duas dimensões.

Tabela 3: Matriz 3x4 - Correlação da ISO 17799 com os modelos COBIT e ITIL

	Operacional	Tático	Estratégico
Controles	- ISO 17799 - COBIT: Entrega e Suporte - COBIT: Aquisição e Implementação	- ISO 17799 - COBIT: Entrega e Suporte	- ISO 17799 - Análise de Risco - COBIT: Auditoria - COBIT: Monitoramento - COBIT: Planejamento e Organização.
Pessoas	- ITIL: Suporte a Serviços (adaptado)	- ITIL: Entrega de Serviços (Expandido)	- COBIT: Auditoria - COBIT: Monitoramento
Processos	- ITIL: Suporte a Serviços (adaptado)	- ITIL: Entrega de Serviços (Expandido)	- COBIT: Auditoria - COBIT: Monitoramento
Tecnologia	- Ferramentas de Workflow - Ferramentas de Gerenciamento (coleta de dados) - Data Warehouse	- Ferramentas de Workflow - Ferramentas de Gerenciamento (coleta de dados) - Data Warehouse - Ferramentas para testes de vulnerabilidade e penetração - Ferramentas para análise de logs	- Ferramentas automatizadas para análise de Risco - Ferramentas automatizadas para a extração de conhecimento

Conforme informado anteriormente, os modelos COBIT e ITIL são utilizados na proposta de um modelo de Governança da Segurança da Informação por possuírem um conjunto de boas práticas definidas para auxiliar a Governança da Tecnologia da Informação. Este conjunto de boas práticas foi desenvolvido a partir de experiências profissionais especialistas que realizam pesquisas por todo o mundo, além de serem utilizados largamente em organizações de todo o mundo nos últimos anos.

A norma ISO 17799 será utilizada como base para o modelo de governança da Segurança da Informação por possuir objetivos de controle específicos e detalhados para o gerenciamento da segurança da informação. Além disto, para ampliar a abrangência da ISO 17799, os objetivos de controle relacionados às melhores práticas para a segurança serão identificados e correlacionados no modelo COBIT. A avaliação em níveis de maturidade proposta pelo COBIT para cada

objetivo de controle irá incorporar à norma ISO 17799 a capacidade de obtenção de um processo contínuo de melhoria da qualidade da segurança computacional dos serviços de TI oferecidos.

Esses objetivos de controle, que são apresentados em alto nível pelo modelo COBIT e de forma detalhada pela norma ISO 17799, deverão ser mapeadas para os processos descritos no modelo ITIL. Dessa forma, este trabalho propõe que o modelo COBIT e a ISO 17799 sejam utilizados para fornecer o que (objetivos de controle) precisa ser implementado, enquanto o modelo ITIL será utilizado para detalhar como isso será feito através de seus processos no nível operacional e tático e ainda, quem será responsável por fazê-lo.

A análise de riscos é proposta para ser realizada no nível estratégico, a fim de auxiliar, com base no planejamento estratégico, os requisitos que deverão ser priorizados e implementados, além do nível de maturidade esperado para cada um. A análise de riscos permitirá aos gestores identificar a necessidade de investimentos para mitigar os riscos envolvidos na execução do planejamento estratégico.

3.7 O NÍVEL OPERACIONAL

O nível operacional descreve atividades necessárias para manter a infra-estrutura de TI em funcionamento. A seguir são detalhadas as dimensões Controle, Processos, Pessoas e Tecnologia para este nível.

3.7.1 Dimensão Controles: Definição dos Objetivos de Controle

Objetivos de Controle presentes no modelo COBIT e identificados neste trabalho para este nível são apresentados na Tabela 4:

Tabela 4: Objetivos de Controle identificados no modelo COBIT para o Nível Operacional

Domínio: Aquisição e Implementação	Domínio: Entrega e Suporte
AI3 – Adquirir e Manter Infra-estrutura Tecnológica	DS5 – Garantir Segurança de Sistemas
AI4 – Desenvolver e Manter Procedimentos	DS7 – Educar e Treinar Usuários
AI5 – Instalar e Validar Sistemas	DS8 – Auxiliar e Aconselhar Clientes
AI6 – Gerenciar Mudanças	DS9 – Gerenciar Configuração
	DS10 – Gerenciar Problemas e Incidentes
	DS11 – Gerenciar Dados
	DS13 – Gerenciar a Operação

Para que possamos maximizar as potencialidades dos objetivos de controle do modelo COBIT, no que se refere à segurança computacional, os objetivos de controle da norma ISO 17799 deverão ser incorporados, conforme descrito anteriormente.

3.7.2 Dimensão Processos: Implementação dos Objetivos de Controle

Os objetivos de controle identificados na norma ISO 17799 e no modelo COBIT serão implementados através de uma adaptação dos processos ITIL de ‘Gerenciamento de Incidentes’, ‘Gerenciamento de Problemas’ e ‘Gerenciamento de Mudanças’ de forma a permitir a reação aos incidentes de segurança computacional no nível Operacional. Assim, para o nível Operacional este trabalho irá propor, para uma futura melhoria, que sejam utilizados os seguintes processos:

- Gerenciamento de Incidentes/Service Desk;
- Gerenciamento de Configurações;
- Gerenciamento de Problemas;
- Gerenciamento de Mudanças;
- Gerenciamento de Versões;

3.7.3 Dimensão Pessoas: Definição de Papéis e Responsabilidades dos Indivíduos Envolvidos

Nesta dimensão, deseja-se apresentar uma documentação clara e objetiva sobre o que é esperado de cada um dos envolvidos com o processo através de uma documentação formal contendo os papéis e responsabilidades para cada indivíduo. A partir de uma análise do detalhamento dos processos do modelo ITIL é possível extrair os indicativos para esta definição.

Uma relação clara de indicadores de performance e fatores críticos de sucesso devem ser definidos para que cada indivíduo possa saber se está cumprindo o que é esperado dentro de todo o processo.

Diante disto, para a definição das responsabilidades e dos papéis de cada indivíduo, os processos do modelo ITIL que poderão ser utilizados para a extração dos indicadores estão presentes no módulo Suporte a serviços, sendo relacionados a seguir:

- Gerenciamento de Incidentes/Service Desk;
- Gerenciamento de Configurações;
- Gerenciamento de Problemas;
- Gerenciamento de Mudanças;
- Gerenciamento de Versões;

3.7.4 Dimensão Tecnologia: Ferramentas de Apoio ao Modelo

Nesta dimensão deverão ser escolhidas as ferramentas para que a implementação do modelo para Governança da Segurança da Informação seja realizada conforme o previsto par o nível operacional do processo de tomada de decisão em sistemas de informações gerenciais. A estrutura de banco de dados

deverá ser definida para armazenar os mais diversos dados provenientes do ambiente e que possam ser relacionados para gerar informação acerca do ambiente a ser protegido.

As bases de dados propostas no modelo ITIL deverão ser consideradas e correlacionadas para a obtenção de um Data Warehouse. Entre as bases de dados que deverão ser propostas para o nível operacional, o modelo ITIL apresenta as seguintes:

- Base de dados para registro de Incidentes;
- Base de dados para registro de problemas;
- Base de dados para Erros conhecidos;
- CMDB (Configuration Management Data Base): Base de Dados dos itens de configuração do ambiente;
- Base de dados para soluções de contorno;

Ferramentas de fluxo de trabalho deverão ser analisadas para fornecer apoio à implantação dos processos previstos para o nível Operacional. Preferencialmente, essas ferramentas deverão possuir a capacidade de registro automático de incidentes a partir de dados coletados por agentes/sensores (por exemplo: agentes SNMP) espalhados pelo ambiente e, ainda, o registro automático dos logs gerados pelos mais diversos sistemas que compõem a infra-estrutura de TI.

3.8 O NÍVEL TÁTICO

O nível tático será responsável pela garantia da qualidade dos serviços de TI oferecidos e pela busca contínua de melhoria dessa qualidade. Para isso, os dados coletados e armazenados no nível operacional serão correlacionados através do

sistema de informação para gerar informações que possam úteis ao incremento do nível de qualidade.

3.8.1 Dimensão Controles: Definição dos Objetivos de Controle

Objetivos de Controle presentes no modelo COBIT e identificados neste trabalho para este nível são os apresentados na Tabela 5:

Tabela 5: Objetivos de Controle identificados no modelo COBIT para o Nível Tático

Domínio: Aquisição e Implementação	Domínio: Entrega e Suporte
AI1 – Identificar Soluções Automatizadas	DS1 – Definir e Gerenciar Níveis de Serviço
AI3 – Adquirir e Manter Infra-estrutura Tecnológica	DS2 – Gerenciar Serviços de Terceiros
AI4 – Desenvolver e Manter Procedimentos	DS3 – Gerenciar Desempenho e Capacidade
AI5 – Instalar e Validar Sistemas	DS4 – Garantir Continuidade dos Serviços
	DS5 – Garantir Segurança de Sistemas
	DS6 – Identificar e Alocar Custos
	DS7 – Educar e Treinar Usuários
	DS8 – Auxiliar e Aconselhar Clientes

Para que possamos maximizar as potencialidades dos objetivos de controle do modelo COBIT, no que se refere à segurança computacional, os objetivos de controle da norma ISO 17799 deverão ser incorporados, conforme descrito anteriormente.

3.8.2 Dimensão Processos: Implementação dos Objetivos de Controle

Este trabalho propõe que objetivos de controle identificados na norma ISO 17799 e no modelo COBIT sejam implementados através dos processos que são alvos da proposta de melhoria, conforme informado anteriormente, através de uma expansão dos processos dos módulos de Suporte a Serviços e Entrega a Serviços com base na incorporação das principais atividades de um CSIRT.

Com essa proposta, pretende-se tornar o modelo ITIL capaz de tratar as particularidades de incidentes de segurança computacional e permitir mais ações pro ativas condizentes com necessidades atuais da infra-estrutura de TI.

Ainda assim, para o nível tático propõe que os seguintes processos sejam utilizados:

- Gerenciamento de Nível de Serviço;
- Gerenciamento de Capacidade;
- Gerenciamento de Continuidade;
- Gerenciamento Financeiro;
- Gerenciamento de Disponibilidade;

3.8.3 Dimensão Pessoas: Definição de Papéis e Responsabilidades dos Indivíduos Envolvidos

Os papéis e responsabilidades para os indivíduos envolvidos no nível tático poderão ser definidos a partir dos indicativos presentes nos processos do modelo ITIL propostos neste trabalho para esse nível. Conforme proposto, os processos ITIL para o nível tático que poderão fornecer esses indicativos são os seguintes:

- Gerenciamento de Nível de Serviço;
- Gerenciamento de Capacidade;
- Gerenciamento de Continuidade;
- Gerenciamento Financeiro;
- Gerenciamento de Disponibilidade;

3.8.4 Dimensão Tecnologia: Ferramentas de Apoio ao Modelo

Assim como na dimensão tecnológica do Nível Operacional, é proposta a utilização ferramentas na dimensão tecnológica no Nível Tático que possam prover: a automação do fluxo de trabalho, tais como ferramentas de workflow, um Data Warehouse e o suporte automatizado ao gerenciamento da infra-estrutura de TI. Essas ferramentas serão utilizadas nessa dimensão para correlacionar os dados obtidos (matéria prima), transformando-os em informações úteis ao processo de melhoria contínua da qualidade da segurança computacional dos serviços providos pela infra-estrutura de TI.

É proposto também que nesta dimensão sejam utilizadas ferramentas automatizadas para a realização de testes de vulnerabilidades e testes de penetração. A partir da informação gerada por essas ferramentas, será possível identificar possíveis vulnerabilidades no ambiente a ser protegido.

Por último, é proposta a utilização de ferramentas automatizadas para análise de eventos, tais como logs que são armazenados como dados brutos no nível operacional. A dificuldade na extração de informação desse tipo de evento é diretamente proporcional ao volume de dados gerados. Dessa forma, a utilização de uma ferramenta automatizada torna-se imprescindível para ajudar na análise em tempo hábil de eventos gerados pelos IDSs, firewalls, ferramentas de gerenciamento, roteadores etc.

3.9 O NÍVEL ESTRATÉGICO

O nível estratégico será responsável por extrair conhecimento das bases de dados que compõem o sistema de informação, promover auditorias e análises de risco e monitorar o ambiente de forma que os gestores da organização possam

incorporar as questões de segurança computacional em suas ações de governança corporativa.

3.9.1 Dimensão Controles: Promover Análise de Risco, Auditoria e Definir Objetivos de Controle

Os objetivos de controle identificados neste trabalho para este nível são apresentados na Tabela 6.

Tabela 6: Objetivos de controle identificados no modelo COBIT para o nível Estratégico.

Planejamento e organização	Monitoramento
PO1– Definir um plano estratégico de TI	ME1 – Monitorar os processos
PO2 – Definir a arquitetura da informação	ME2 – Avaliar a adequação do controle interno
PO3 – Determinar a direção tecnológica	ME3 – Obter certificação independente
PO4 – Definir a Organização e Relacionamentos de TI	ME4 – Providenciar Auditoria Independente
PO5 – Gerenciar o Investimento em TI	
PO6 – Comunicar metas e diretivas gerenciais	
PO7 – Gerenciar Recursos Humanos	
PO8 – Garantir Conformidade com Requisitos Externos	
PO9 – Avaliar Riscos	
PO10 – Gerenciar Projetos	
PO11 – Gerenciar Qualidade	

Nesta dimensão, além de fornecer os objetivos de controle, o modelo COBIT será utilizado para prover um guia de auditoria para avaliações periódicas desses objetivos de controle.

Uma Análise de Risco deverá ser realizada para permitir que os gestores tenham conhecimento acerca dos riscos existentes que podem comprometer a realização da missão da organização. Este conhecimento guiará o gestor no nível de investimento ideal para cada objetivo de controle identificado.

3.9.2 Dimensão Processos: Auditoria e Monitoração dos Processos estabelecidos

Todos os processos precisam ser regularmente avaliados ao longo do tempo em relação à sua qualidade e conformidade com os controles exigidos. Nessa dimensão serão utilizados os objetivos de controle fornecidos pelo COBIT para Monitoramento e suas diretrizes de auditoria para permitir uma auditoria interna ou externa.

3.9.3 Dimensão Pessoas: Auditar e Monitorar as Atividades Exercidas pelos Indivíduos

Assim como na dimensão de processos, a auditoria também deve ser aplicada às pessoas. O conhecimento gerado a partir da auditoria irá guiar a organização numa tentativa de reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações.

3.9.4 Dimensão Tecnologia: Facilitar Análise de Risco e Extração de Conhecimento

A Análise de Risco, caso seja realizada internamente pela organização, deverá ter o suporte de um conjunto de ferramentas automatizadas, de forma a padronizar a sua execução e a facilitar a consolidação dos resultados. As ferramentas corretas deverão ser identificadas e disponibilizadas no momento da auditoria. Essas ferramentas vão desde planilhas eletrônicas com formulários de análise de Risco até ferramentas totalmente automatizadas com capacidade de coleta de dados e extração de conhecimento de base de dados.

Uma vez estruturado o sistema de informação, uma metodologia de extração de conhecimento de base de dados dever ser aplicada. A escolha dessas ferramentas para a realização da análise de riscos está relacionada com a estrutura de Data Warehouse estabelecido para o nível operacional e para o nível tático.

4 VANTAGENS E LIMITAÇÕES DO MODELO PROPORSTO

Conforme informado anteriormente, os requisitos definidos pelo Corporate Governance Task Force buscam atender empresas de diferentes portes, segmentos e com necessidades distintas.

Todavia, nota-se uma facilidade maior na adoção do modelo de Governança da Segurança da Informação proposto neste trabalho em empresas de grande porte, indiferente de seu segmento de mercado, por geralmente possuírem uma área de Segurança da Informação já fortemente estabelecida e consolidada.

Isso se deve ao fato de empresas de pequeno e médio porte concentrar seus investimentos em produtos e/ou serviços que as possibilitem aumentar o seu Market Share, reduzir os custos de produção, aumentar sua linha de produtos e/ou serviços etc. Diante deste cenário, a responsabilidade de garantir a Segurança da Informação é atribuída geralmente á área de TI, que ainda é vista como uma área de custos do que como um diferencial competitivo e fazendo com que a Segurança da Informação seja tratada apenas como uma questão técnica, através da implementação de Firewall, antivírus, IDS etc.

Além disto, o modelo propõe a adoção de um Data Warehouse como fonte de extração do conhecimento necessário ao gestor para o planejamento estratégico da organização. Em empresas de grande porte o Data Warehouse é facilmente encontrado devido à grande quantidade de sistemas que são utilizados na organização, ao enorme volume de dados que são armazenados nestes sistemas e da necessidade de obter respostas cada vez mais rápidas e consistentes, através do processo de tomada de decisão, ao negócio.

Em empresas de pequeno e médio porte, entretanto, a existência de um Data Warehouse não é tão comum, pois a sua implementação não é uma simples questão de tecnologia de base de dados ou processadores atuando paralelamente. Implementar um Data Warehouse envolve planejamento e modelagem (que são aspectos muitas vezes deixados em segundo plano, mas que garantem a qualidade dos dados, que é um fator crítico para o sucesso), integração de diferentes produtos de software e uma contínua atualização e refinamento.

Diante desta complexidade, a implementação desta tecnologia demanda um alto investimento financeiro, onde se encontra uma elevada taxa percentual do faturamento destas organizações. Além disto, estas empresas geralmente não possuem um grande número de sistemas e os volumes de dados armazenados não são tão elevados, fazendo com que a que a relação custo x benefício não seja inicialmente favorável.

Com isto, empresas de pequeno e médio porte, que não contam com o auxílio de um Data Warehouse, utilizam-se dos relatórios gerenciais de todos os sistemas que suportam os seus negócios para a tomada de decisão.

Porém isto não impede que empresas de pequeno e médio porte, que possuam uma área de Segurança da Informação independente da área de TI, também possam adotar o modelo proposto de Governança da Segurança da Informação. Neste caso, é indicado que seja realizada inicialmente uma análise de riscos em toda, ou em parte da organização. A definição de um bom escopo permitirá otimizar os custos e maximizar as implementações dos controles de segurança nas áreas e/ou processos mais críticos da organização, de forma a minimizar os riscos nos quais estão expostos.

Através dos resultados obtidos na avaliação dos riscos, processo no qual são avaliados os indicadores identificados durante a análise, será possível identificar, direcionar e a priorizar as ações gerenciais mais adequadas aliada à capacidade de investimentos, além poder definir o grau de maturidade dos objetivos de controle implementados de acordo com as necessidades da organização. É extremamente importante que os resultados identificados nestes processos sejam apresentados à alta direção, de forma a fazerem parte do planejamento estratégico das organizações no processo de tomada de decisão.

Uma vez que os processos mais críticos da organização alcançarem o nível de maturidade desejada, é aconselhável que o escopo da análise de risco seja ampliada, de forma a garantir a implementação dos objetivos de controle nos demais processos.

A seguir são apresentadas as vantagens e as limitações da adoção do modelo de Governança da Segurança da Informação proposto neste trabalho.

4.1 VANTAGENS

A principal vantagem na adoção do modelo de Governança da Segurança da Informação é o alinhamento estratégico aos negócios, permitindo que a segurança da informação deixe de ser tratada apenas como uma questão técnica, passando a ser um desafio estratégico e administrativo, como parte integrante das “melhores práticas corporativas”, não deixando de cobrir aspectos relacionados com as pessoas, processos e tecnologia.

Além disto, o modelo proposto permitirá o uso combinado dos modelos COBIT, ITIL e da norma ISO 17799. Esses modelos já são utilizados amplamente no mundo, porém de forma isolada. O grande diferencial deste trabalho está na

combinação do que cada modelo possui de melhor, criando uma solução customizada, capaz de atender às demandas de negócio de cada organização.

Além disto, a ISO 17799, considerada atualmente o padrão internacional mais completo para o gerenciamento de segurança da informação nas organizações, serve como uma bússola para a implementação e manutenção do Sistema de Gestão da Segurança da Informação.

Em adicional, a adoção deste modelo, ainda no âmbito da ISO 17799, permitirá que as organizações se preparem para a certificação. Uma vez certificada, a organização demonstrará a sua adequação e a maturidade em segurança da informação, trazendo um grande diferencial competitivo, uma vez que atualmente as empresas buscam parceiros de negócio que estejam comprometidos com este tema.

Já COBIT, constitui uma importante ferramenta na estruturação e no controle dos processos de TI de forma a atender a demanda das diversas áreas da empresa, dos acionistas, dos órgãos regulatórios e das entidades externas, por alinhamento, transparência e equalização dos riscos de TI.

O COBIT foi criado com as características para ser focado no negócio da empresa e é totalmente orientado aos processos e às medições de maturidade com base em controles. Fornece informações detalhadas para gerenciar os processos baseados em objetivos de negócios.

Alguns exemplos demonstram as vantagens da implementação do COBIT, tais como, suporta e é suportado pelas melhores práticas, provendo assim um ambiente de TI bem gerenciado e flexível, foca na melhoria da Governança de TI das organizações e na redução dos riscos operacionais, gerencia e controla as atividades de TI, proporciona um ambiente de controle responsável em garantir as

necessidades de negócio, disponibiliza ferramentas para auxiliar no gerenciamento e no controle das atividades de TI, garante que as funções corporativas ocorram de forma sistemática para o alcance dos objetivos do negócio e cria uma linguagem comum para todos os envolvidos nos controles dos processos.

Quanto ao ITIL, ao ser implementado em uma organização, a área de TI deixa de ser vista apenas como um departamento, mas como parte integrante do negócio.

Alguns exemplos demonstram as vantagens da implementação do ITIL, tais como, a facilidade de gerenciamento de serviços de TI e, conseqüentemente, de toda a empresa, oferece uma linha de trabalho consistente, padronizada e eficiente, realiza uma redução, em longo prazo, dos custos dos serviços prestados, melhora o processo de comunicação entre funcionários, parceiros e clientes da empresa e aumenta a satisfação de todos os envolvidos, ao definir corretamente as metas e expectativas.

4.2 LIMITAÇÕES

Conforme verificado, o modelo de Governança da Segurança da Informação proposto neste trabalho apresentou uma adoção melhor em empresas de grande porte, por contarem com uma área de Segurança da Informação definida, consolidada, atuando em conjunto com a alta direção e fazendo parte do planejamento estratégico, de forma a garantir que a segurança não se restrinja apenas no âmbito tecnológico.

Além disto, através do correlacionamento dos objetivos de controle presentes no modelo COBIT e na norma ISO 17799 com os processos descritos no modelo ITIL identificou-se que os módulos de Suporte a Serviços e Entrega de

Serviços do modelo ITIL não estão estruturados para implementar todos os objetivos de controle apresentados para o nível Operacional e Tático.

Para que o modelo ITIL seja capaz de implementar todos os objetivos de controle apresentados pela norma ISO 17799 e pelo modelo COBIT para os níveis operacional e tático, deve-se realizar uma expansão dos processos de Gerenciamento de Incidentes, Gerenciamento de Problemas e Gerenciamento de Mudanças, além da inserção de um novo processo chamado de Gerenciamento de Comportamento, no nível tático.

Apesar de o modelo ITIL ter a capacidade de tratar incidentes de forma reativa (Gerenciamento de Incidentes) e de forma pro ativa (Gerenciamento de Problemas e Gerenciamento de Mudanças), ambos no nível operacional, torna-se necessário essa expansão tendo em vista as particularidades de um incidente de segurança computacional e a necessidade de implementar os objetivos de controle previstos no modelo COBIT e na norma ISO 17799.

5 CONCLUSÃO

Este trabalho propôs um modelo para Governança da Segurança da Informação que se baseia na Estrutura de Decisão dos Sistemas de Informações Gerenciais (SIGs) e através do correlacionamento dos modelos COBIT e ITIL e da norma ISO 17799.

As necessidades de tratar a Segurança Computacional não apenas no âmbito tecnológico, mas de alcançar um modelo onde o conhecimento esteja disponível de forma objetiva para o conselho administrativo ao longo de todo o processo de tomada de decisão para a execução do negócio, conduziu este trabalho a considerar as questões de Governança da Tecnologia da Informação.

Para o desenvolvimento do modelo de Governança da Segurança da informação foram utilizados os 13 requisitos mínimos propostos pelo Corporate Governance Task Force, uma vez que atendem a empresas de diferentes portes, segmentos e com necessidades distintas. Esses requisitos foram mapeados numa estrutura matricial (matriz 3x4) que contempla os níveis de decisão (operacional, tático e estratégico) e as dimensões que amparam cada um desses níveis de decisão (Controle, Processos, Pessoas e Tecnologia).

Considerando essa estrutura matricial, que possui uma abrangência ampla, foi possível o desenvolvimento de um modelo que permite o alinhamento estratégico entre Segurança Computacional e o Negócio da Organização.

O modelo apresentado considerou a utilização das melhores práticas dos modelos de apoio à Governança de TI em função desses modelos terem sido desenvolvidos por especialistas, testados e implementados por uma grande quantidade de organizações ao redor do mundo.

A estrutura matricial do modelo desenvolvido irá permitir a definição de níveis de maturidade isoladamente para controles, processos, pessoas e tecnologia em cada um dos níveis de decisão. Isso facilitará a evolução do modelo e permitirá que as falhas sejam atacadas de forma pontual.

A combinação do modelo COBIT com a norma ISO 17799 e o modelo ITIL permitirá a utilização das potencialidades de cada uma dessas propostas para o desenvolvimento de um modelo único que facilite identificar: o que, quem, como e que recursos tecnológicos utilizar para o alcance da Governança da Segurança da Informação.

Além disto, de forma a ampliar abrangência do modelo proposto, sugere-se uma adaptação dos processos ITIL de 'Gerenciamento de Incidentes', 'Gerenciamento de Problemas' e 'Gerenciamento de Mudanças', para que esses processos permitam a reação aos incidentes de segurança computacional no nível operacional, além do desenvolvimento de um novo processo para o nível tático.

Apesar de o modelo ITIL ter a capacidade de tratar incidentes de forma reativa (Gerenciamento de Incidentes) e de forma pro ativa (Gerenciamento de Problemas e Gerenciamento de Mudanças), ambos no nível operacional, torna-se necessário essa expansão tendo em vista as particularidades de um incidente de segurança computacional e a necessidade de implementar os objetivos de controle previstos no modelo COBIT e na norma ISO 17799. Todavia estas soluções apresentam-se como proposta de melhoria deste trabalho.

6 REFERÊNCIAS

ABNT. **Tecnologia da Informação – Código de Prática para a gestão da segurança da informação.** NBR ISO/IEC 17799, 2001.

ALVES, G. A. **Segurança da Informação: uma visão inovadora da gestão.** Rio de Janeiro: Ciência Moderna, 2006.

BIO, S. R. **Sistemas de Informação: um enfoque gerencial.** São Paulo: Atlas, 1994.

CAMPOS, A.L.N. **Sistema de Segurança da Informação: Controlando os Riscos.** Florianópolis: Visual Books, 2005.

CORPORATE GOVERNANCE TASK FORCE REPORT. **Information Security Governance: A call to action.** Abril, 2004. Disponível on-line em: http://www.cyberpartnership.org/infosecgov4_04.pdf. Visitado em 23/02/2008.

OLIVEIRA, D. P. R. **Sistemas de Informações Gerenciais.** 5. ed. São Paulo: Atlas, 1998.

ONLINE ETYMOLOGY DICTIONARY. Disponível on-line em: http://www.etymonline.com. Visitado em 04/09/2007.

SÊMOLA, M. **Gestão da Segurança da Informação.** Rio de Janeiro: Campos, 2003.

7 BIBLIOGRAFIA

ENTRUST. **Information Security Governance (ISG): An Essential Element of Corporate Governance.** Abril, 2004. Disponível on-line em: http://www.entrust.com/governance/. Visitado em 23/02/2008.

Office of Government Commerce (OGC). **ITIL: The Key to Managing IT Services – Best Practice for Security Management.** Printed in the United Kingdom for the Stationery Office, 2001.

Office of Government Commerce (OGC). **ITIL: The Key to Managing IT Services – Best Practice for Service Delivery.** Printed in the United Kingdom for the Stationery Office, 2001.

THE IT GOVERNANCE INSTITUTE. **COBIT: Control Objectives for Information and Related Technology.** Printed in the United States of America, 2000.

THE IT GOVERNANCE INSTITUTE. **Information Security Governance: Guidance for Boards of Directors and Executive Management.** Printed in the USA, 2001. Disponível on-line em: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6672. Visitado em 23/02/2008.